SU-ICT-03-2018: Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap

Specific Challenge: EU's strategic interest is to ensure that the EU retains and develops essential capacities to secure its digital economy, infrastructures, society, and democracy. Europe's cybersecurity research, competences and investments are spread across Europe with too little alignment. There is an urgent need to step up investment in technological advancements that could make the EU's digital Single Market more cybersecure and to overcome the fragmentation of EU research capacities. Europe has to master the relevant cybersecurity technologies from secure components to trustworthy interconnected IoT ecosystems and to self-healing software. European industries need to be supported and equipped with latest technologies and skills to develop innovative security products and services and protect their vital assets against cyberattacks. This should contribute inter alia to achieve the objective of European strategic autonomy.

The Public Private Partnership on Cybersecurity[1] created in 2016 was an important first step aiming at triggering up to EUR 1.8 billion of investment. However, the scale of the investment under way in other parts of the world suggests that the EU needs to do more in terms of investment and overcome the fragmentation of capacities spread across the EU. In this context in a recent Joint Communication[2] the Commission announced the intention to create a Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre.

Scope: The objective of this topic is to scale up existing research for the benefit of the cybersecurity of the Digital Single Market, with solutions that can be marketable. For this, participants should in parallel propose, test, validate and exploit the possible organisational, functional, procedural, technological and operational setup of a cybersecurity competence network with a central competence hub. Projects under this topic will help build and strengthen cybersecurity capacities across the EU as well as provide valuable input for the future set-up of the Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre as mentioned by the Joint Communication.

To achieve the above, support will go to consortia of competence centres in cybersecurity to engage together in:

- Common research, development and innovation in next generation industrial and civilian cybersecurity technologies (including dual-use), applications and services; focus should be on horizontal cybersecurity technologies as well as on cybersecurity in critical sectors (e.g. energy, transport, health, finance, eGovernment, telecom, space, manufacturing);
- Strengthening cybersecurity capacities across the EU and closing the cyber skills gap;

[1] C(2016) 440 final

[2] Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN (2017) 450 final

- Supporting certification authorities with testing and validation labs equipped with state of the art technologies and expertise.

Each proposal should bring together cybersecurity R&D&I centres in Europe (e.g. university labs/public or private non-profit research centres) to create synergies and scale up existing competences and demonstrated strengths to the European level. Proposals should take into consideration relevant active digital ecosystems and public-private cooperation models and focus on solving technological and industrial challenges. The centres within the proposal should aim to collectively develop and implement a Cybersecurity Roadmap covering the above and addressing multiple and complementary cybersecurity disciplines (e.g. cryptography, network security, application security, IoT/cloud security, data integrity and privacy, secure digital identities, security/crisis management, forensic technologies, security investigation, cyber psychology, bio-security). When developing the Roadmap the results of the work done by the cPPP on cybersecurity, notably its Strategic Research and Innovation Agenda, will serve as a starting point. Consideration should also be given to the relevant work of ENISA, Europol and other EU agencies and bodies.

The Roadmap should include targets to be achieved with deliverables by the end of the project (typically three to four years) that constitute clear milestones in its implementation, as well as priorities to be addressed in the future by the Cybersecurity Competence Network.

To implement this Roadmap, partners in the proposal(s) are expected to set up a functional network of centres of expertise with a coordinating "competence centre" (this role should be undertaken by one of the partners in the network, with the necessary capacity, resources and experience). Work includes the assessment of various organisational and legal solutions for the Cybersecurity Competence Network, taking into account various criteria, including the EU mechanisms and rules, national and regional funding structures, as well as those offered by industry. Based on the above work, a governance structure should be proposed (i.e. business model, operational and decision-making procedures/processes, technologies and people) and will be implemented, tested and validated in the demonstration cases (see below) involving all partners in the network to showcase (in a measurable manner) its performance and optimise the suggested governance structure.

Projects will demonstrate the effectiveness of their selected governance structure by providing collaborative solutions to enhance cybersecurity capacities of the network and develop cyber skills (e.g. by looking at models to align cybersecurity curricula at graduate/post graduate levels; align cybersecurity certification programmes; classify skills with work roles).

Projects should ensure outreach, to raise knowledge and awareness of cybersecurity issues among a wider circle of professionals, where possible in cooperation with EU and national efforts, and to spread the developed expertise.

Projects should also include industrial partners and their cybersecurity research collaborators to create synergies and: (a) collaboratively identify and analyse scalable (short/mid/long

term[3]) cybersecurity industrial challenges in the selected sectors and (b) demonstrate their ability to collaborate in developing appropriate solutions to solve critical challenges through (not less than four) research and innovation demonstration cases.

These demonstration cases will constitute the core part of the work to be done within the project. They will be based on a specific research & development roadmap to tackle selected industrial challenges and will implement it covering a complete range of activities, from research & innovation through testing, experimentation and validation to certification activities.

Projects under this topic are implemented as a programme through the use of complementary grants. The respective options of Article 2, Article 31.6 and Article 41.4 of the Model Grant Agreement will be applied. Proposals shall therefore foresee resources for clustering activities with other projects funded under this topic to identify synergies, best practices and kick-off the process of creating the network involving the sub-networks already created by awarded projects. This task will contribute to the actual set-up of the Cybersecurity Competence Network and a European Cybersecurity Research and Competence Centre at a later stage.

A proposal must involve distinct cybersecurity R&D&I excellence centres in Europe (e.g. university labs, public or private non-profit research centres, taking into consideration public-private cooperation models and the ecosystems around them), with complementary expertise, from at least 9 Member States or Associated Countries. With the aim of reinforcing technology and industrial capacity as widely as possible across Europe, proposals should include a substantial representation of the most relevant RD&I excellences centres in Europe, with a widespread European coverage and good geographical balance of activities as regards the scope of work. This will ensure the proposals meeting the policy goals of the initiative of supporting the establishment of the future Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre of the European Union.

The consortium in a proposal must involve at least 20 partners.

A proposal should also include industrial partners from various (not less than 3) sectors (e.g. telecom, finance, transport, eGovernment, health, space, defence, manufacturing) that will be involved in the demonstration cases.

The support and involvement of the relevant governmental bodies and authorities (e.g. for monitoring and assessing the projects' results during their life-cycles) will be considered as an asset.

The Commission considers that proposals requesting a contribution of up to EUR 16 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

---

[3] *Short term*: referring to cybersecurity challenges in existing industrial products that can be addressed by the research and computational capabilities of the Network, *medium term*: referring to cybersecurity challenges in upcoming products that can be addressed by the research and computational capabilities of the Network and the Center and *long term*: high risk research for challenges that will shape new policies for long-term innovation capabilities requiring computational and research capacities beyond the existing ones by the Network.

For grants awarded under this topic the Commission may object to a transfer of ownership or the exclusive licensing of results to a third party established in a third country not associated to Horizon 2020. The respective option of Article 30.3 of the Model Grant Agreement will be applied.

Under this call topic, the beneficiaries nominated as project coordinators cannot, in this capacity, be awarded more than one grant from the European Union budget. In case an applicant organisation appears as coordinator in more than one proposal, only the last submitted proposal will be considered for evaluation. This approach should allow different governance models to be tested through this topic and provide a wide range of complementary outcomes, including lessons learnt, for the future set-up.

Expected Impact:

- Cybersecurity solutions, products or services for the identified critical challenges, increasing the cybersecurity of the Digital Single Market , in particular for sectors from which stakeholders are involved;
- A feasible, sustainable governance model for the Cybersecurity Competence Network developed and tested through successful pilot projects addressing selected industrial challenges;
- Clearly demonstrated strengthening of Member States' research and innovation competence and cybersecurity capacities, also within their national cybersecurity ecosystems, to meet the increasing cybersecurity challenges;
- Synergies between experts from various cybersecurity domains demonstrated;
- Bridges built between the network and industrial communities;
- Research and Development programme with a common Research and Innovation Roadmap reflecting all different cybersecurity sectors and covering a wide range of activities from research to testing;
- A cybersecurity skills framework model developed, which can be used as a reference by education providers to develop appropriate curricula; by employers, to help assess their cybersecurity workforce, and improve job descriptions; by citizens to reskill themselves;
- Establishment of foundations for pooling and streamlining the development and deployment of cybersecurity technology and strengthening industrial capabilities to secure EU's digital economy, society, democracy, space and infrastructures.

Type of Action: Research and Innovation action